УДК 519.61:511-33

К ВОПРОСУ СУЩЕСТВОВАНИЯ МАТРИЦ МЕРСЕННА И АДАМАРА

Н. А. Балонин,
доктор техн. наук, профессор
Санкт-Петербургский государственный университет аэрокосмического приборостроения
М. Б. Сергеев,
доктор техн. наук, профессор
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Рассматриваются условия существования матриц Мерсенна. На примере анализа условий существования матриц Белевича показано, что ограничения, характерные для целочисленных матриц, не сказываются на матрицах с рациональными и иррациональными значениями уровней, к которым принадлежат матрицы Мерсенна. Приводится зависимость значений уровней от порядка матрицы Мерсенна, показывается отсутствие особых точек на графике этой зависимости. Комментируется связь гипотез существования матриц Адамара и Мерсенна.

Ключевые слова *— ортогональные матрицы, матрицы Адамара, матрицы Белевича, матрицы Мерсенна, М-матрицы, гипотеза существования.*

Введение

Предпосылки доказательства существования матриц Мерсенна рассмотрены в работе [1] в связи с найденными матрицами 11-го и 19-го порядков, выходящих за пределы основной последовательности порядков $n=2^k-1$ [2].

Напомним, что матрица Мерсенна $\mathbf{M}_n$ [1] — это квадратная матрица порядка $n=4k-1$ с элементами $\{1, -b\}$ такая, что $\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n = \mu\,\mathbf{I}_n$. Здесь $\mathbf{I}_n$ — единичная матрица; $\mu=\dfrac{(n+1)+(n-1)b^2}{2}$, причем $b=\dfrac{1}{2}$ при $n=3$, в остальных случаях $b=\dfrac{q-\sqrt{4q}}{q-4}$, где $q=n+1$. Количество элементов $-b$ в каждом столбце матрицы на единицу меньше количества единичных элементов.

Интерпретация теоремы Гилмана

Порядки $n=4k-1$ возникают в теории смежных с ними матриц Адамара [3]. В частности, из теоремы Гилмана [4] следует, что матрица Адамара порядка n существует, если $n-1$ — простое число.

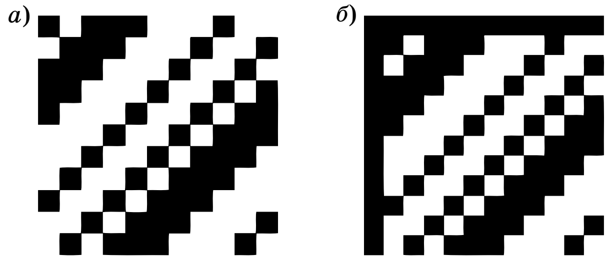
В приложении к матрицам Мерсенна теорема Гилмана звучит проще: матрица Мерсенна существует, если ее порядок — простое число.

В самом деле, для порядков 3, 7, 11, 19 матрицы Мерсенна существуют [1], причем матрица Адамара 12-го порядка ($\mathbf{H}_{12}$) получается из матрицы $\mathbf{M}_{11}$ округлением ее отрицательных элементов до значения –1 с добавлением каймы в виде строки и столбца с отрицательными элементами для соблюдения баланса положительных и отрицательных элементов. Иллюстрацией сказанного является рис. 1, *а*, *б*, где черный цвет соответствует $-b$ (или –1), а белый — единице.

Обратим внимание: матрица $\mathbf{M}_{15}$ не удовлетворяет условию теоремы Гилмана, однако ее порядок принадлежит к последовательности $n=2^k-1$, для которой известен алгоритм построения матриц. Это означает, что теорема Гилмана касается не столько существования матриц Мерсенна и Адамара, сколько гарантии нахождения матриц некоторой относительно простой структуры. Портреты матриц отражают общую идею перехода от матриц Мерсенна к матрицам Адамара (и обратно).

Критерий существования матриц Белевича

Из матриц, на два порядка меньших матриц Адамара и тоже тесно связанных с ними, известны матрицы Белевича $\mathbf{C}_n$ [5] — квадратные ма-



■ *Рис. 1.* Портреты матриц Мерсенна $\mathbf{M}_{11}$ (*а*) и Адамара $\mathbf{H}_{12}$ (*б*)

трицы порядков n с элементами {1, –1} и нулевой диагональю такие, что

$$\mathbf{C}_n^{\mathrm{T}}\mathbf{C}_n = (n-1)\,\mathbf{I}_n. \qquad (*)$$

Известно, что они не существуют для значений $n-1$, не разложимых в сумму квадратов двух целых чисел.

Разберем подробнее доказательство этого утверждения.

Выражение (*) можно рассматривать в обратном порядке как условие разложения целочисленного для этих матриц весового коэффициента $w=n-1$ на суммы квадратов элементов вектор-столбцов матриц $\mathbf{C}_n$. Про суммы квадратов известна теорема Лагранжа, из которой следует, что всякое целое число может быть представлено суммой четырех квадратов натуральных чисел [6]. Количество слагаемых в отмеченной сумме, в общем, избыточно и может быть сокращено без изменения значения весового коэффициента в правой части (*) итерационным удалением каймы матрицы, представляемой блочно в виде

$$\mathbf{C}=\begin{pmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{G} & \mathbf{D}\end{pmatrix}.$$

Алгоритм Лагранжа. Выражение $\mathbf{C}=\mathbf{D}-\mathbf{G}(\mathbf{A}-\mathbf{W})^{-1}\mathbf{B}$ описывает процедуру понижения порядка n матрицы удалением блоков $\mathbf{A}$, $\mathbf{B}$, $\mathbf{G}$ с коррекцией элементов блока $\mathbf{D}$, где $\mathbf{W}$ — квазиортогональная матрица с тем же весом $\mathbf{W}^{\mathrm{T}}\mathbf{W}=w\mathbf{I}$.

От порядка матриц $\mathbf{A}$, $\mathbf{W}$ зависит количество удаляемых на шаге алгоритма слагаемых. Невырожденность их разности $(\mathbf{A}-\mathbf{W})$ с учетом свободы смены знака элементов строк и столбцов $\mathbf{W}$ обеспечивает, например, конструкция Вильямсона

$$\mathbf{W}=\begin{pmatrix} w_1 & w_2 & w_3 & w_4\\ -w_2 & w_1 & -w_4 & w_3\\ -w_3 & w_4 & w_1 & -w_2\\ -w_4 & -w_3 & w_2 & w_1\end{pmatrix}$$

с четырьмя коэффициентами, удовлетворяющими условию $w_1^2+w_2^2+w_3^2+w_4^2=w$. Итерационное применение алгоритма понижения порядка n с сохранением веса w формально сводит его к порядку 2.

Пример. Этапы понижения порядка матрицы Белевича с 6-го до 2-го при выборе $w_1=2$, $w_2=1$, $w_3=0$ и $w_4=0$ отражены ниже. Для того чтобы не вводить новые обозначения, обозначим финальную матрицу как $\mathbf{C}_2$, хотя она выйдет из класса матриц с преимущественно единичными по норме коэффициентами:

$$\mathbf{C}_6=\begin{pmatrix}0 & 1 & 1 & 1 & 1 & 1\\ 1 & 0 & 1 & -1 & -1 & 1\\ 1 & 1 & 0 & 1 & -1 & -1\\ 1 & -1 & 1 & 0 & 1 & -1\\ 1 & -1 & -1 & 1 & 0 & 1\\ 1 & 1 & -1 & -1 & 1 & 0\end{pmatrix};$$

$$\mathbf{C}_6^{\mathrm{T}}\mathbf{C}_6=\begin{pmatrix}5 & 0 & 0 & 0 & 0 & 0\\ 0 & 5 & 0 & 0 & 0 & 0\\ 0 & 0 & 5 & 0 & 0 & 0\\ 0 & 0 & 0 & 5 & 0 & 0\\ 0 & 0 & 0 & 0 & 5 & 0\\ 0 & 0 & 0 & 0 & 0 & 5\end{pmatrix};$$

$$\mathbf{C}_2=\begin{pmatrix}-1 & 2\\ 2 & 1\end{pmatrix};\quad \mathbf{C}_2^{\mathrm{T}}\mathbf{C}_2=\begin{pmatrix}5 & 0\\ 0 & 5\end{pmatrix}.$$

Поскольку элементы матрицы Белевича исходно целочисленные, а инверсия $(\mathbf{A}-\mathbf{W})$ базируется на операциях алгебраического сложения, умножения и деления чисел, то соблюдаемое на каждом шаге алгоритма постоянство значения w означает выражение числа $n-1$ суммой квадратов двух целых или, в общем, рациональных чисел. Для того чтобы разобраться, когда такое равенство возможно, необходимо напомнить следующие две теоремы.

Согласно *теореме Эйлера*, нечетное простое число представимо в виде суммы двух квадратов (целых чисел) тогда и только тогда, когда оно имеет вид $4k+1$. В иностранной литературе это утверждение часто называют рождественской теоремой Ферма, так как она стала известна из письма Пьера Ферма Марену Мерсенну, посланного 25 декабря 1640 года. Из этой теоремы выводится общее утверждение: натуральное число представимо в виде суммы двух квадратов (целых чисел) тогда и только тогда, когда любое простое число вида $4k+3$ входит в его разложение на простые множители в четной степени. Иногда именно это утверждение считается *теоремой Эйлера — Ферма*.

Отсюда следует, что если сумма двух квадратов рациональных чисел равна целому числу, то оно разложимо и на сумму квадратов целых чисел. Применительно к рассматриваемой задаче это означает, что если значение $n-1$ не разложимо на сумму двух квадратов, то матрицы, сводимой к матрице 2-го порядка, не существует. Это и есть формулировка необходимого критерия существования матриц Белевича. Если нет матриц Белевича, то невозможно построить матрицы Адамара, базирующиеся на них (детали комментировались в работах [5, 7] и некоторых других).

Применение алгоритма Лагранжа к матрицам Мерсенна

Алгоритм Лагранжа индифферентен к виду слагаемых — он может оперировать и с исходно иррациональными числами, гарантируя всего лишь то, что с ними будут производиться те же операции, что и в случае матриц Белевича. Тем самым весовой коэффициент μ матриц Мерсенна формально может быть сведен к сумме трех квадратов.

Пример. Последовательность приведения матрицы 7-го порядка к матрице 3-го порядка отражена ниже. Здесь $q=n+1=8$; $b=\frac{q-\sqrt{4q}}{q-4}\cong 0{,}586$; $\mu=\frac{(n+1)+(n-1)b^2}{2}\cong 5{,}029$; $w_1=\sqrt{\mu}$; $w_2=0$; $w_3=0$; $w_4=0$.

$$\mathbf{M}_7=\begin{pmatrix} 1 & -b & -b & -b & 1 & 1 & 1\\ -b & 1 & -b & 1 & 1 & -b & 1\\ -b & -b & 1 & 1 & -b & 1 & 1\\ -b & 1 & 1 & -b & 1 & 1 & -b\\ 1 & 1 & -b & 1 & -b & -b & -b\\ 1 & -b & 1 & 1 & 1 & -b & -b\\ 1 & 1 & 1 & -b & -b & -b & 1 \end{pmatrix};$$

$$\mathbf{M}_7^{\mathrm{T}}\mathbf{M}_7=\begin{pmatrix} \mu & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & \mu & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & \mu & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & \mu & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \mu & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \mu & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \mu \end{pmatrix};$$

$$\mathbf{M}_3=\begin{pmatrix} 2{,}243 & 0 & 0\\ 0 & 2{,}243 & 0\\ 0 & 0 & 2{,}243 \end{pmatrix};\quad \mathbf{M}_3^{\mathrm{T}}\mathbf{M}_3=\begin{pmatrix} \mu & 0 & 0\\ 0 & \mu & 0\\ 0 & 0 & \mu \end{pmatrix}.$$

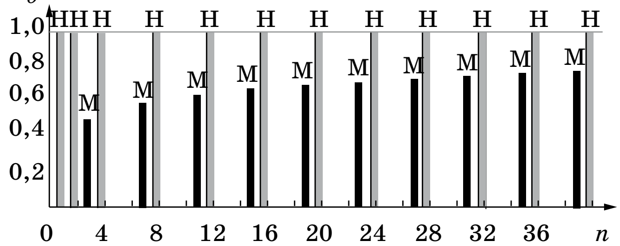
Известно, что целое число разложимо на сумму трех квадратов, если оно не принадлежит к виду $4^m(8k+7)$. Столь подробный анализ, впрочем, излишен — случаи, когда значение элемента b матрицы не приводимо к рациональному виду, установить проще, поскольку для его вычисления получена прямая формула. Соответственно, применение алгоритма Лагранжа к матрицам Мерсенна, в отличие от предыдущего случая, не вскрывает наличия противоречия, которое не позволило бы им существовать.

Отсутствие особых точек на графике уровня элементов

Начиная с теоремы Гилмана и некоторых других, сходных, анализ возможности существования матриц Адамара нередко подменяется вопросом об области применимости того или иного алгоритма их построения или существования какой-либо особой их разновидности. Такая постановка не совсем правомерна. Так, например, вопрос о существовании корней полиномов был решен положительно (при изменении области их определения с вещественной оси на комплексную плоскость), в то же время, как известно, общей формулы для нахождения корней полиномов высоких порядков нет.

В отличие от целочисленных матриц Адамара и Белевича, матрицы Мерсенна определены на более широком классе: когда вариант рациональных значений их коэффициентов невозможен (как у матриц Белевича), он восполняется решением с иррациональными числами. Зависимость коэффициентов b матриц Мерсенна от порядка n не содержит особых точек, свидетельствующих об отсутствии матриц (рис. 2).

В случае, когда придется констатировать отсутствие существования матриц Мерсенна, возникнет вопрос о том, что же тогда, согласно этой зависимости, вычислялось? В теме существования матриц Мерсенна довольно много такого рода нюансов. Можно и так рассуждать: решения ли-



■ *Рис. 2.* Зависимость уровней матриц Мерсенна **M** и Адамара **H** от порядка n

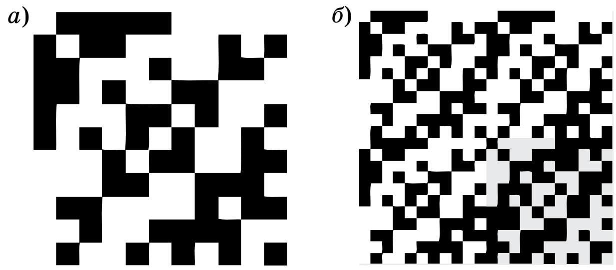
нейных дифференциальных уравнений, например, имеют ограниченное количество особенностей, в силу чего их параметры можно найти, располагая конечным числом точек интегральной кривой (а не всей кривой). Если матрицы Мерсенна, вопреки зависимости $b(n)$ (см. рис. 2), не существуют, придется объяснять характер причудливой избирательности, для проявления которой в постановке иной, независимой задачи, как видится, нет оснований.

В самом деле, помимо определения матриц Мерсенна заданием вида правой части выражения (*), существует оптимизационный подход, при котором матрицы Мерсенна определяются как частные случаи минимаксных М-матриц [8, 9]. Оба этих независимых между собой подхода приводят к одинаковому результату в отношении формулы для нахождения модуля их уровня b, но во втором случае вид правой части (*) является предметом поиска, т. е. свободен. Решение следует из соблюдения условий ортогональности, а широкая область определения матриц создает предпосылки для разрешимости. Если бы задача изначально не рассматривалась как чисто комбинаторная, то, возможно, соображения по существованию необходимых ортогональных базисов появились бы раньше, поскольку для ортогональных матриц с любым значением элементов задача не является сколь-нибудь выделенной.

Семейство матриц Адамара

Рассматриваемый выше анализ поднимает более глубокий вопрос о принадлежности квазиортогональных матриц к семейству, частными проявлениями которого являются матрицы Адамара [3], Мерсенна [1, 2], Эйлера [10] и Ферма [11]. Матрицы перечислены в последовательности убывания переменной d в значении порядка $n=4k-d$, где $d=0$, 1, 2, 3. Случай $d=0$ (матрицы Адамара) известен в научной литературе достаточно давно, и для него получен ряд алгоритмов, например, Скарпи [12], Пэли [13] и др. Случаи матриц нечетных порядков, а также некоторых четных изучены недостаточно полно.

При понижении значения порядка ортогональность столбцов матрицы достигается увеличением количества уровней — значений, которым равны элементы матрицы (или их модули). Матрицы Адамара — одноуровневые по модулям элементов матрицы, матрицы Мерсенна — двухуровневые, матрицы Эйлера — четырехуровневые (с учетом знака) матрицы. Порядки $n=4k-3$ исследованы менее всего, для них известна последовательность матриц Адамара — Ферма [11]. Матрицы эти расположены ближе к матрицам Адамара на единицу меньших порядков $n-1$ и



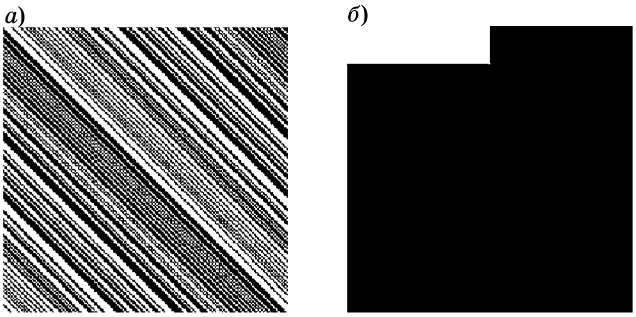
■ *Рис. 3.* Портреты матриц $\mathbf{M}_{11}$ (*а*) и $\mathbf{E}_{22}$ (*б*)

наследуют от них всего лишь трехуровневую структуру. Вне пределов основной зависимости такого вида матриц нет. Можно предположить, что есть и другие виды матриц на этих порядках, тяготеющие к матрицам Эйлера.

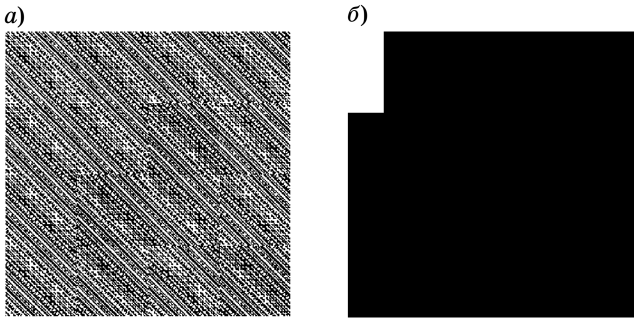
Матрица Эйлера 22-го порядка ($\mathbf{E}_{22}$), невозможного для матриц Белевича (число 21 не разлагается на сумму двух квадратов), напротив, существует, так как она получается из матрицы $\mathbf{M}_{11}$ (рис. 3, *а*, *б*) простым применением алгоритма Сильвестра [1]. Это значит, что существуют связанные с ней матрицы $\mathbf{M}_{23}$ и $\mathbf{H}_{24}$. Об отложенной для матриц $\mathbf{H}_{44}$ проблеме, как в случае с симметричными матрицами Белевича, это также не свидетельствует, поскольку есть связанная с ней матрица $\mathbf{M}_{43}$. Таким образом, матрицы Белевича порядков $n=4k-2$ принадлежат не к слою, а к побочной ветви матриц, из которых матрицы Адамара удвоенного порядка иногда строятся, иногда нет. На критическом $n=22$ экстремальное значение детерминанта на классе квазиортогональных матриц достигается не на них, а на иных структурах [14, 15].

Для известных в теории матриц Адамара случаев, когда не находится алгоритм построения (отличный от переборного), матрицы Мерсенна существуют; в частности, это касается матрицы $\mathbf{M}_{91}$, соответствующей первой найденной перебором на компьютере матрице $\mathbf{H}_{92}$, ее невозможно построить методом Пэли [13]. Помимо Пэли, и как раз в связи с недостатками его подхода, блочное построение матриц Адамара исследовано Вильямсоном [6]. Поскольку, согласно алгоритму Лагранжа, их можно находить при помощи конструкции $\mathbf{W}$, он предложил заменить в ней четыре скалярных коэффициента четырьмя попарно-коммутативными симметричными матрицами вчетверо меньших, чем у матриц Адамара, порядков.

Возникающая отсюда комбинаторная задача по перебору целочисленных элементов блочных матриц Вильямсона трудоемка и не всегда может быть решена существующими средствами. В таких случаях стоит задуматься о приближениях, поскольку каков бы ни был порядок следующей



■ *Рис. 4.* Портрет матрицы $\mathbf{M}_{167}$ и гистограмма модулей ее элементов



■ *Рис. 5.* Портрет матрицы приближения к $\mathbf{H}_{668}$ и гистограмма модулей ее элементов

найденной перебором матрицы, проблема этим только отодвигается. Об этом материал следующего раздела.

Приближение матриц Адамара матрицами Мерсенна

Случаи, для которых производительность современных вычислительных машин не позволяет пока вычислить матрицы Адамара методом Вильямсона, достаточно хорошо известны — это порядки 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964 и т. п. [16]. Заметим, что вчетверо меньшие значения порядков — это порядки матриц Мерсенна. Так как матрицы Адамара относительно небольших порядков давно изучены, это открывает определенные перспективы для их применения трансформацией их в матрицы Мерсенна.

Например, в качестве четырех матриц Вильямсона возьмем первую из них — матрицу Мерсенна (или Эйлера), а остальные три — ее же, но с округленными до значений {1, –1} коэффициентами. Так как остается одна степень свободы влиять на ортогональность столбцов полученной таким способом матрицы учетверенного порядка (выбором значения варьируемого коэффициента b неокругленной матрицы), оказывается, что этот метод позволяет находить квазиортогональные матрицы без характерного для метода Вильямсона перебора: совместность гарантируется структурой.

Стартовые матрицы $\mathbf{M}_3$ и $\mathbf{E}_6$ переходят сразу в матрицы $\mathbf{H}_{12}$ и $\mathbf{H}_{24}$.

В общем случае зависимость $b(n)$ *и*меет особую точку — $n=44$ (для матриц Мерсенна) и $n=88$ (для матриц Эйлера), где она меняет свой знак. Для порядков, меньших, чем отмеченные особо, матрицы Адамара можно найти примерно так же, как это делается в методе Пэли с матрицами Белевича — доопределением модулей элементов до единицы и сменой знака части элементов.

Матрицы более высоких порядков проще оставлять такими, каковы они есть, что существенно упрощает алгоритм исключением наиболее трудоемкой операции — перебора. Например, матрица Мерсенна относительно малого 167-го порядка, судя по гистограмме ее уровней, немногим отличается уже от матрицы Адамара (рис. 4, *а*, *б*).

При использовании $\mathbf{M}_{167}$ в конструкции Вильямсона коэффициент b, характеризующий приближение к матрице $\mathbf{H}_{668}$, составляет около 70 % от максимально возможного уровня, и элементов с уровнем, отличным от единицы, становится заметно меньше в относительном соотношении (рис. 5, *а*, *б*). У остальных матриц перечисленных выше порядков он еще больше — приближается к единице с ростом n.

Использование матриц Вильямсона с матрицами Мерсенна, разумеется, не единственное приложение матриц Мерсенна. Везде, где возникают их характерные порядки, уверенно можно полагать, что они принимают в расчетах действенное участие. Так, например, при вычислении матрицы Адамара порядка $(n-1)n$ по матрице Адамара порядка n (метод Скарпи [12]) фигурирует размерность матриц Мерсенна. Этот метод значительно проще интерпретируется как вставка матрицы Мерсенна в саму себя с каймой у блочных матриц, равной по знаку значению вытесняемого и округляемого до единицы элемента. Так как в оригинальном методе нет элементов b, столь простая формулировка и сам взгляд на решение как специфическое квадрирование матриц Мерсенна, а не матриц Адамара, в нем невозможны.

Данный подход позволяет находить матрицы, недостижимые методом Пэли [13]. Кроме того, он указывает на характер замены известного кронекерова произведения матриц Адамара при переходе к матрицам Мерсенна.

Исследование слоев матриц, т. е. матриц, заданных для характерных им порядков функциями уровней, помимо достижения более полного понимания проблемы, позволяет находить оригинальные неизвестные ранее методы вычисления матриц Адамара или новых их приближений с помощью нецелочисленных матриц Мерсенна. Для ряда приложений квазиортогональных матриц к помехоустойчивому кодированию информации и маскированию изображений целочисленные значения их элементов далеко не столь важны, как важна высокая размерность решаемой задачи и наличие экстремальных качеств [8], которыми обладают матрицы Адамара и все близкие к ним матрицы их семейства.

Заключение

В настоящей работе исследованы условия существования предложенных авторами матриц Мерсенна. На примере анализа условий существования матриц Белевича показано, что ограничения, характерные для этих целочисленных матриц, не сказываются на матрицах с рациональными и, в общем, иррациональными значениями уровней, к которым принадлежат матрицы Мерсенна. Вместе с тем нецелочисленные коэффициенты матриц Мерсенна не мешают искать впоследствии целочисленную матрицу Адамара, поскольку от иррациональной матрицы наследуется только ее структура.

Перспектива решения проблемы Адамара длительное время связывалась с успешностью комбинаторных алгоритмов их нахождения. Никакой частный алгоритм, разумеется, не способен эту очевидно большую задачу — поиска матриц Адамара любого порядка — решить. Если принять во внимание преемственность слоев семейства матриц, включающих и матрицы Адамара, то, учитывая их связанность, возможна общая схема доказательства факта существования всех таких матриц. Она не обязывает уметь находить сами матрицы, а опирается на возможность указать функции, описывающие их уровни. Причем эти функции не имеют особых точек, свидетельствующих о неопределенности. Принадлежность матриц к слою и наличие одного или более слоев расценивается, как раз, по наличию функций уровней, описывающих слой.

Матрицы Мерсенна предпочтительнее матриц Адамара потому, что они занимают в тетраде матриц Адамара, Мерсенна, Эйлера, Ферма наиболее удаленное положение от матриц порядка $4k-3$, на котором наблюдается отсутствие явно выделенного и проходящего по всем порядкам матриц слоя. Справа и слева (по порядкам) от матриц Мерсенна находятся связанные с ними взаимно-однозначным соответствием матрицы Адамара и Эйлера. Компромиссное (не целое) значение уровня b отличает этот слой от слоя родственных им матриц Адамара. На порядках матриц Ферма решение, согласно общей логике построения этих матриц, связано с образованием дополнительных уровней, — это не параметрическое, а более сложное структурное изменение матрицы.

Хотя множества матриц в соседствующих слоях равновелики по количеству их представителей, исследовать условия разрешимости задачи проще на порядках $4k-1$, делая соответствующие выводы в отношении побочных представителей. Роль особых точек в зависимости $b(n)$ подчеркивается еще тем, что для конструкций Вильямсона, например, особые точки связаны с принципиальной возможностью или невозможностью с их помощью находить матрицы Адамара. Это некоторая дополнительная информация, которая отсутствует в альтернативном подходе.

О влиянии иррациональных чисел на разрешимость проблемы нахождения матриц Белевича, а значит, и матриц Адамара, известно давно. Стоит отметить, что основной и оригинальный результат Пэли связан с примером построения символов Лежандра для конечного поля $FG(9)$ с иррациональными значениями элементов, поскольку 9 — не простое число. Матрица Белевича 10-го порядка имеет вложенные структуры, в которых несложно идентифицируются матрицы Мерсенна 3-го порядка. С помощью матриц нечетного порядка эта задача (и сходные) решается, возможно, менее элегантно, без привлечения теории конечных полей, но методически более просто.

В том случае, когда матрица Мерсенна найдена, она непосредственно приводит к матрице Адамара на единицу большего порядка. Таким образом, гипотезы о существовании матриц некоторых четных (впервые предположение высказал, скорее всего, не Адамар, а Пэли, комментируя ограниченность алгоритмов, впоследствии используемых в теории матриц Белевича) [13] и нечетных значений порядков [1] взаимно связаны, обнаруживают родство при поисках доказательства и дополняют друг друга.

Литература

1. **Балонин Н. А.** О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2. С. 89–90.
2. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Мерсенна // Информационно-управляющие системы. 2012. № 5. С. 92–94.
3. **Hadamard J.** Résolution d'une question relative aux determinants // Bulletin des Sciences Mathématiques. 1893. Vol. 17. P. 240–246.

4. **Gilman R. E.** On the Hadamard determinant theorem and orthogonal determinants // Bull. Amer. Math. Soc. 1931. Vol. 37. P. 30–31.
5. **Belevitch V.** Theorem of 2n-terminal networks with application to conference telephony // Electr. Commun. 1950. Vol. 26. P. 231–244.
6. **Williamson J.** Hadamard's Determinant Theorem and the Sum of Four Squares // Duke Math. J. 1944. Vol. 11. P. 65–81.
7. **Van Lint J. H., Seidel J. J.** Equilateral point sets in elliptic geometry // Indagationes Mathematicae. 1966. Vol. 28. P. 335–348.
8. **Балонин Н. А., Сергеев М. Б.** М-матрицы // Информационно-управляющие системы. 2011. № 1. С. 14–21.
9. **Балонин Ю. Н., Сергеев М. Б.** Алгоритм и программа поиска и исследования М-матриц // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3. С. 82–86.
10. **Балонин Н. А., Сергеев М. Б.** О двух способах построения матриц Адамара — Эйлера // Информационно-управляющие системы. 2013. № 1. С. 7–10.
11. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Ферма // Информационно-управляющие системы. 2012. № 6. С. 90–93.
12. **Scarpis U.** Sui determinanti di valore Massimo // Rendiconti della R. Istituto Lombardo di Scienze e Lettere. 1898: 31. P. 1441–1446.
13. **Paley R. E. A. C.** On orthogonal matrices//J. of Mathematics and Physics. 1933. Vol. 12. P. 311–320.
14. **Балонин Ю. Н., Сергеев М. Б.** М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87–90.
15. **Балонин Н. А., Сергеев М. Б.** Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке // Информационно-управляющие системы. 2013. № 5. С. 97–98.
16. **Shalom Eliahou.** La conjecture de Hadamard (I) — Images des Mathématiques // CNRS. 2012. http://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (дата обращения: 15.08.2013).